(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
29 août 2002 (29.08.2002)

PCT

(10) Numéro de publication internationale
WO 02/067534 A1

(51) Classification internationale des brevets[7] : H04L 29/06, 9/32

(21) Numéro de la demande internationale : PCT/FR02/00626

(22) Date de dépôt international : 19 février 2002 (19.02.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/02262 20 février 2001 (20.02.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **MOBILEWAY** [FR/FR]; 4, avenue Hoche, F-75008 Paris (FR).

(72) Inventeurs; et

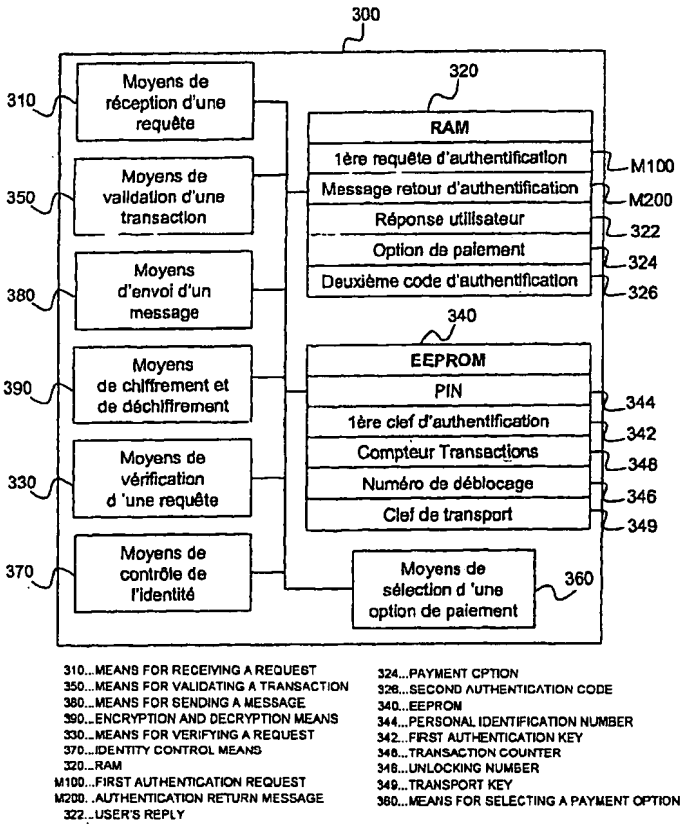
(75) Inventeurs/Déposants *(pour US seulement)* : **DOLIQUE, Christophe** [FR/FR]; 16-22, rue du Tertre, F-92150 Suresnes (FR). **BARBIER, Eric** [FR/FR]; 44, rue de Lagny, F-75020 Paris (FR). **GUILLOT, Carles** [FR/FR]; 26bis, rue Charles Baudelaire, F-75012 Paris (FR).

(74) Mandataire : **CABINET BONNET-THIRION**; 12, avenue de la Grande Armée, B.P. 966, F-75829 Paris Cedex 17 (FR).

[Suite sur la page suivante]

(54) Title: REMOTE ELECTRONIC PAYMENT SYSTEM

(54) Titre : SYSTEME DE PAIEMENT ELECTRONIQUE A DISTANCE



(57) Abstract: The invention concerns a remote electronic payment system comprising an authentication device (300) with an authenticating server in a remote payment system, the authentication being performed prior to a transaction carried out by a user. The device (300) is characterised in that it comprises: means (310) for receiving a first authentication request, from the authenticating server; means (330) for verifying the validity of the authentication request; means (350) for validation, by the user, of the transaction; means (370) for controlling said user's identity; and means (380) for sending a return message of authentication, to the authenticating server (900).

(57) Abrégé : Ce système de paiement électronique à distance comporte un dispositif d'authentification (300) auprès d'un serveur d'authentification dans un système de paiement à distance, l'authentification étant préalable à une transaction par un utilisateur, le dispositif (300) étant caractérisé en ce qu'il comporte: -des moyens (310) de réception d'une première requête d'authentification, en provenance du serveur d'authentification; -des moyens (330) de vérification de la validité de la requête d'authentification; -des moyens (350) de validation, par l'utilisateur, de la transaction; -des moyens (370) de contrôle de l'identité dudit utilisateur ; et -des moyens (380) d'envoi d'un message retour d'authentification, vers le serveur d'authentification (900).

WO 02/067534 A1

(81) **États désignés** *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

"Système de paiement électronique à distance"

La présente invention concerne un système de paiement électronique à distance.

L'invention vise notamment un dispositif d'authentification auprès d'un serveur d'authentification dans un système de paiement à distance, permettant de déclencher des transactions à partir d'un téléphone portable.

Il n'existe actuellement pas de procédé permettant d'authentifier un utilisateur préalablement à une opération de paiement à distance qui s'affranchisse d'un lecteur de carte à puce.

Par ailleurs, dans une première catégorie connue d'appareils électroniques permettant de réaliser des transactions à distance, il est demandé à l'utilisateur de saisir des références d'un moyen de paiement, tel qu'une carte de crédit. Ces références sont, de façon connue, cryptées et transmises au fournisseur distant.

De tels appareils électroniques doivent comporter une interface utilisateur permettant une saisie facile de ces références. Ce n'est en particulier pas le cas pour les téléphones portables, dont le clavier et l'écran sont généralement de taille réduite.

On connaît également des téléphones portables comportant un lecteur de carte de crédit intégré. Cette solution permet effectivement de supprimer la saisie des références précitées. Elle permet en outre une authentification préalable à une opération de paiement. Mais cette solution nécessite en revanche des composants complexes et coûteux.

Il apparaît de plus que la plupart des consommateurs hésitent à fournir les références d'un moyen de paiement à leur fournisseur, qui plus est à travers un réseau de communication.

On connaît également, dans le domaine du commerce électronique sur Internet, des systèmes de paiement électronique à distance, pour lesquels les références d'un moyen de paiement sont stockées sur un serveur appelé portefeuille électronique (« server based electronic wallet » en anglais). Dans un tel système, l'utilisateur s'authentifie auprès du serveur

portefeuille électronique distant, depuis un terminal client, par exemple un ordinateur personnel (« PC ») comportant des moyens d'authentification, typiquement intégrés à un butineur Internet (« Internet browser » en anglais).

La plupart des téléphones portables, en particulier ceux ne comportant pas de butineur Internet, ne fournissent pas de tels moyens d'authentification. Les téléphones portables qui mettent en œuvre le protocole WAP ("Wireless Access Procol" en anglais) ne fournissent pas non plus de tels moyens. Ils ne peuvent donc pas servir de terminal client permettant à un utilisateur de s'authentifier auprès d'un serveur portefeuille électronique.

La présente invention a pour but de résoudre ce problème, en proposant en particulier un dispositif d'authentification adapté à être incorporé dans un téléphone portable.

Dans ce but, la présente invention propose un dispositif d'authentification auprès d'un serveur d'authentification dans un système de paiement à distance, l'authentification étant préalable à une transaction par un utilisateur, le dispositif étant caractérisé en ce qu'il comporte :

-des moyens de réception d'une première requête d'authentification, en provenance du serveur d'authentification ;

-des moyens de vérification de la validité de la requête d'authentification ;

-des moyens de validation, par l'utilisateur, de la transaction ;

-des moyens de contrôle de l'identité de l'utilisateur ; et

-des moyens d'envoi d'un message retour d'authentification, vers le serveur d'authentification.

Corrélativement, l'invention a pour objet un procédé d'authentification auprès d'un serveur d'authentification dans un système de paiement à distance, l'authentification étant préalable à une transaction par un utilisateur, le procédé étant caractérisé en ce qu'il comporte les étapes suivantes :

-réception d'une première requête d'authentification, en provenance du serveur d'authentification ;

-vérification de la validité de la requête d'authentification ;

-validation, par l'utilisateur, de la transaction ;

-contrôle de l'identité de l'utilisateur ; et

-envoi d'un message retour d'authentification, vers le serveur d'authentification.

Les caractéristiques particulières et les avantages du procédé d'authentification étant similaires à ceux du dispositif d'authentification, ils ne sont pas énumérés ici.

Ainsi, l'invention permet tout d'abord d'authentifier l'utilisateur avant la validation de la transaction. De plus, l'envoi du message retour d'authentification se fait après une vérification de la validité de la requête d'authentification. Cette mesure permet de s'assurer que le message retour d'authentification n'est pas envoyé à un destinataire mal intentionné.

Selon une caractéristique particulière, la requête d'authentification comprend une description de la transaction, un identifiant de la transaction et un premier code d'authentification du serveur d'authentification, les moyens de vérification du dispositif d'authentification étant adaptés à vérifier la validité de la requête d'authentification à partir du premier code d'authentification et d'une première clef d'authentification.

Ce mécanisme à clef d'authentification permet de vérifier, avec une excellente fiabilité, la validité de la requête d'authentification.

Selon une autre caractéristique particulière, le dispositif d'authentification comporte en outre des moyens de génération d'un deuxième code d'authentification, les moyens d'envoi du message retour d'authentification étant adaptés à insérer ce deuxième code d'authentification dans le message retour d'authentification.

Ce mécanisme permet, au niveau du serveur d'authentification, de s'assurer que le message retour d'authentification provient effectivement du dispositif d'authentification.

Selon une caractéristique préférée, les moyens d'envoi du message retour d'authentification sont adaptés à insérer une réponse fonction de la validation de la transaction dans le message retour d'authentification.

Le message retour d'authentification pourra par exemple contenir des données représentatives de l'acceptation de la transaction par l'utilisateur, qui pourront être transmises par le serveur d'authentification à un établissement financier.

Selon une caractéristique préférée, les moyens de contrôle de l'identité de l'utilisateur utilisent un numéro d'identification personnel.

Ce numéro d'identification personnel, que l'utilisateur aura par exemple reçu par courrier, empêchera l'utilisation du dispositif d'authentification par un tiers. De façon connue, les moyens de contrôle de l'identité de l'utilisateur peuvent par exemple être adaptés à bloquer le dispositif d'authentification après trois saisies d'un numéro d'identification personnel erroné.

Selon une caractéristique préférée, le dispositif d'authentification comporte en outre des moyens de déchiffrement de la première requête d'authentification à partir d'une clef de transport, et/ou des moyens de chiffrement du message retour d'authentification à partir d'une clef de transport.

Cette caractéristique avantageuse augmente considérablement la confidentialité de la transaction.

Selon une autre caractéristique, la transaction comportant une opération de paiement, le dispositif comporte des moyens de sélection d'une option de paiement de la transaction et les moyens d'envoi du message retour d'authentification sont adaptés à insérer cette option dans le message retour d'authentification.

Ceci permet en particulier d'offrir un service de paiement électronique à distance indépendant d'une option de paiement. Il est même tout à fait envisageable que ces moyens de paiement soient virtuels, ou dédiés à ce service de paiement électronique à distance. Même piratés, ils ne sont dans ce cas d'aucune utilité pour un utilisateur mal intentionné, ce qui renforce encore la sécurité du système.

Selon une autre caractéristique particulière, le dispositif d'authentification comporte en outre un compteur de transactions utilisé par les moyens de génération et du deuxième code d'authentification et inséré par les

moyens d'envoi du message retour d'authentification dans le message retour d'authentification.

Cet identificateur permet ainsi d'identifier, de manière unique, chaque message retour d'authentification.

Selon une autre caractéristique particulière, le dispositif d'authentification comporte des moyens de réception, en provenance d'un serveur d'activation, d'un message de livraison de clefs, le message de livraison de clefs comportant la première clef d'authentification.

La clef d'authentification est ainsi fournie par un serveur, de préférence de façon transparente pour l'utilisateur, ce qui permet de renforcer la sécurité du système.

Selon une autre caractéristique particulière, le message de livraison de clefs comporte en outre un numéro d'identification personnel de déblocage.

De façon classique, ce numéro d'identification personnel de déblocage est utilisé pour débloquer le dispositif d'authentification lorsque celui-ci a été bloqué, par exemple après trois saisies d'un numéro d'identification personnel erroné.

Selon une autre caractéristique particulière, le dispositif d'authentification comporte en outre des moyens de vérification de la validité du message de livraison de clefs, à partir d'un troisième code d'authentification contenu dans le message de livraison de clefs.

L'invention vise également un serveur d'activation, dans un système de paiement à distance, caractérisé en ce qu'il comporte :

-des moyens de réception d'une requête d'activation en provenance d'un serveur de comptes d'utilisateurs, la requête d'activation comportant un identificateur d'un dispositif d'authentification tel que décrit ci-dessus ;

-des moyens de génération de la première clef d'authentification ; et

-des moyens d'envoi, sur réception d'une réponse à la requête d'activation, du message de livraison de clefs au dispositif d'authentification.

La génération de la clef d'authentification est ainsi sous la responsabilité du serveur d'activation.

Selon une caractéristique particulière, l'identificateur est un numéro de téléphone.

Selon une autre caractéristique particulière, le serveur d'activation comporte en outre des moyens de sauvegarde de la première clef d'authentification dans une base de données sécurisée.

Le serveur d'activation garde ainsi une copie de la première clef d'authentification. Cette clef pourra être transmise ultérieurement à un serveur d'authentification qui pourra mettre en œuvre un mécanisme d'authentification à clef symétrique (en anglais « Symmetrical Key Infrastructure ») avec le dispositif d'authentification.

Selon une autre caractéristique, le serveur d'activation comporte des moyens de génération d'une deuxième clef d'authentification, à partir de la première clef d'authentification, et comporte des moyens de sauvegarde de cette deuxième clef d'authentification dans la base de données sécurisée.

Cette deuxième clef pourra alors être transmise ultérieurement à un serveur d'authentification qui pourra mettre en œuvre un mécanisme d'authentification à clef asymétrique avec le dispositif d'authentification.

Selon une autre caractéristique particulière, le serveur d'activation comporte des moyens de calcul d'un troisième code d'authentification, ce troisième code d'authentification étant inséré dans le message de livraison de clefs.

Ce mécanisme permet au dispositif d'authentification de s'assurer de la validité du message de livraison de clefs.

Selon une autre caractéristique particulière, le serveur d'activation insère un numéro d'identification personnel de déblocage dans le message de livraison de clefs.

Comme décrit précédemment, ce numéro d'identification personnel de déblocage est utilisé pour débloquer le dispositif d'authentification lorsque celui-ci a été bloqué, par exemple après trois saisies d'un numéro d'identification personnel erroné.

Selon une autre caractéristique particulière, le serveur d'activation comporte en outre des moyens de chiffrement du message de livraison de clefs, à partir d'une clef de transport.

Cette caractéristique avantageuse augmente considérablement la confidentialité du message d'activation.

Selon une autre caractéristique particulière, le serveur d'activation comporte en outre des moyens d'obtention de la clef de transport et d'un numéro d'identification personnel de déblocage à partir d'une base de données de pré-activation.

Cette clef de transport peut en outre être utilisée pour le calcul du troisième code d'authentification.

Cette base de données de pré-activation est typiquement une base de données générique, mise à jour pour chaque création d'un dispositif d'authentification. Cela permet en particulier à l'opérateur du système de paiement de garder une maîtrise sur les dispositifs d'authentification.

Selon une autre caractéristique particulière, le serveur d'activation comporte des moyens d'envoi d'un enregistrement d'authentification, à destination d'un serveur d'authentification, l'enregistrement d'authentification comportant la clef de transport et le numéro d'identification personnel de déblocage.

Le serveur d'authentification possèdera ainsi la clef de transport lui permettant d'échanger, de façon sécurisée, les messages relatifs aux transactions avec le dispositif d'authentification.

Corrélativement, l'invention vise un serveur de comptes utilisateurs, dans un système de paiement à distance, caractérisé en ce qu'il comporte :

- des moyens de création et de stockage d'au moins un compte utilisateur associé à un dispositif d'authentification tel que décrit ci-dessus ;
- des moyens d'envoi d'une requête d'activation, à destination d'un serveur d'activation tel que décrit ci-dessus ; et
- des moyens d'envoi d'une deuxième requête d'authentification à destination d'un serveur d'authentification.

Un compte utilisateur est ainsi créé pour tout utilisateur en possession d'un dispositif d'authentification tel que décrit ci-dessus et désirant effectivement utiliser (par exemple via un abonnement) un tel système de paiement électronique à distance. Après création de ce compte, le serveur de comptes utilisateurs envoie une requête d'activation à destination du serveur d'activation qui génère et fournit la clef d'authentification à l'utilisateur.

Selon une caractéristique particulière, un compte utilisateur comporte un identificateur du dispositif d'authentification (par exemple un numéro de téléphone) et au moins une option de paiement de la transaction.

L'invention vise aussi un serveur d'authentification, dans un système de paiement à distance, caractérisé en ce qu'il comporte :

-des moyens de réception d'au moins un enregistrement d'authentification en provenance d'un serveur d'activation tel que décrit ci-dessus ;

-des moyens de stockage de l'enregistrement d'authentification ;

-des moyens de réception d'une deuxième requête d'authentification en provenance d'un serveur de comptes utilisateurs tel que décrit ci-dessus ;

-des moyens d'envoi de la première requête d'authentification, à destination d'un dispositif d'authentification tel que décrit ci-dessus, à réception de la deuxième requête d'authentification ;

-des moyens de réception d'un message retour d'authentification, en provenance du dispositif d'authentification ; et

-des moyens d'envoi d'un message de confirmation de transaction au serveur de comptes utilisateurs, sur réception du message retour d'authentification.

Un tel serveur d'authentification reçoit ainsi, à l'activation du service, un enregistrement d'authentification contenant la clef de transport et le numéro d'identification personnel de déblocage associés à un dispositif d'authentification. Pour chaque transaction, il reçoit alors une requête d'authentification provenant d'un serveur de comptes utilisateurs. Il peut alors envoyer une première requête d'authentification à un dispositif d'authentification

incorporé dans un terminal client, et recevoir en retour une validation de la transaction de l'utilisateur ainsi qu'un moyen de paiement. Ces dernières informations sont ainsi transmises dans un message de confirmation de transaction au serveur de comptes utilisateurs qui termine la transaction proprement dite.

Corrélativement, l'invention vise un système de paiement à distance, caractérisé en ce qu'il comporte un dispositif d'authentification, un serveur d'activation, un serveur de comptes utilisateurs et un serveur d'authentification tels que décrits ci-dessus.

Selon une caractéristique particulière, le système de paiement à distance utilise une infrastructure d'un réseau de téléphonie mobile, par exemple celle d'un réseau GSM.

Un dispositif d'authentification peut ainsi être incorporé dans un terminal client mobile.

Selon une autre caractéristique particulière, les messages et requêtes décrits ci-dessus sont conformes au format SMS du réseau GSM.

Cette caractéristique permet avantageusement de ne pas développer un protocole de communication spécifique pour le déploiement d'un tel service de paiement électronique à distance.

L'invention vise aussi une carte à puce et une carte SIM comportant un dispositif d'authentification tel que défini ci-dessus.

Ceci permet avantageusement d'utiliser les moyens de chiffrement et de déchiffrement de la carte SIM, traditionnellement dédiés au chiffrement et au déchiffrement de messages de télécommunication, pour le chiffrement et le déchiffrement de messages associés à un paiement électronique à distance.

L'invention vise également un téléphone comportant des moyens adaptés à recevoir une carte SIM telle que définie ci-dessus.

Ainsi, un tel téléphone peut ainsi être utilisé comme terminal client d'authentification auprès d'un serveur portefeuille électronique.

Selon une caractéristique particulière, le téléphone selon la comporte en outre des moyens de saisie du numéro d'identification personnel.

Ainsi, et de façon connue, l'utilisateur peut saisir son numéro d'identification personnel, ce numéro ayant été par exemple reçu par courrier en confirmation de l'abonnement.

D'autres aspects et avantages de la présente invention apparaîtront plus clairement à la lecture de la description de modes particuliers de réalisation qui va suivre, cette description étant donnée uniquement à titre d'exemple non limitatif et faite en référence aux dessins annexés sur lesquels :

-la figure 1 représente schématiquement une requête d'authentification selon l'invention, dans un mode particulier de réalisation ;

-la figure 2 représente un message retour d'authentification selon l'invention, dans un mode particulier de réalisation ;

-la figure 3 représente un dispositif d'authentification selon l'invention, dans un mode particulier de réalisation ;

-la figure 4 représente un message de livraison de clefs selon l'invention, dans un mode particulier de réalisation ;

-la figure 5 représente un serveur d'activation selon l'invention, dans un mode particulier de réalisation ;

-la figure 6 représente une requête d'activation selon l'invention, dans un mode particulier de réalisation ;

-la figure 7 représente un enregistrement d'authentification selon l'invention, dans un mode particulier de réalisation ;

-la figure 8 représente un serveur de comptes utilisateurs selon l'invention, dans un mode particulier de réalisation ;

-la figure 9 représente un serveur d'authentification selon l'invention, dans un mode particulier de réalisation ;

-la figure 10 représente un système de paiement électronique à distance selon l'invention, dans un mode particulier de réalisation ; et

-la figure 11 représente un organigramme d'un procédé d'authentification selon l'invention, dans un mode particulier de réalisation.

La **figure 1** représente une requête d'authentification M100 selon l'invention. Une telle requête d'authentification M100 comporte un premier champ M110 comportant les détails d'une transaction. Ces détails sont par

exemple les références d'un fournisseur, le montant de la transaction et différentes options de paiement 831, 832 illustrées sur la figure 8.

La requête d'authentification M100 comporte un deuxième champ M120 d'identification de la transaction, par exemple sous la forme d'un numéro de transaction. Elle comporte enfin un premier code d'authentification M130. Ce premier code d'authentification M130 permet de s'assurer que la requête d'authentification M100 a été émise par un serveur d'authentification valide.

La **figure 2** représente un message retour d'authentification M200 selon l'invention. Une tel message retour d'authentification M200 comporte un premier champ M210 de réponse utilisateur, représentatif de l'acceptation ou du rejet de la transaction décrite dans le champ M110 d'une requête d'authentification M100.

Le message retour d'authentification M200 comporte également un champ M220 contenant une option de paiement de la transaction. Ce champ est bien entendu utile uniquement dans le cas où le champ réponse utilisateur M210 est représentatif de l'acceptation de la transaction.

Le message retour d'authentification comporte également, dans un champ M230, la valeur d'un compteur de transactions 348 tel que décrit ultérieurement en référence à la figure 3.

Le message retour d'authentification M200 comporte enfin un deuxième code d'authentification dans un champ M240, ce code étant similaire au premier code d'authentification M130 de la requête d'authentification M100.

La **figure 3** représente un dispositif d'authentification 300 selon l'invention. Le dispositif d'authentification 300 comporte des moyens 310 de réception d'une requête d'authentification M100 comme décrit en référence à la figure 1. Ces moyens de réception 310 sont adaptés à stocker la requête d'authentification M100 reçue dans une mémoire vive 320 (RAM).

Le dispositif d'authentification 300 comporte des moyens 330 de vérification de la validité de la requête d'authentification M100. Ces moyens utilisent en particulier le premier code d'authentification M130 contenu dans la requête d'authentification M100 et une première clef d'authentification 342 stockée dans un registre d'une mémoire non volatile (EEPROM) 340.

Cette première clef d'authentification 342 est par exemple reçue en provenance d'un serveur d'activation 500 tel que décrit ultérieurement en référence à la figure 5. Le procédé mis en œuvre par les moyens de vérification 330 sont connus de l'homme du métier et ne seront pas décrits ici. Ces moyens de vérification 330 sont bien entendu adaptés à vérifier toute autre requête reçue par le dispositif d'authentification 300 et en particulier une requête d'activation M600 telle que décrite ultérieurement en référence à la figure 6.

Le dispositif d'authentification 300 comporte des moyens 350 de validation d'une transaction. Ces moyens sont par exemple adaptés à afficher les détails de la transaction contenus dans le champ M110 de la requête M100 et à recueillir une réponse utilisateur 322 représentative de l'acceptation ou du rejet de la transaction par l'utilisateur. Cette réponse utilisateur 322 est stockée dans la RAM 320 par les moyens 350 de validation d'une transaction.

Le dispositif d'authentification 300 comporte également des moyens 360 de sélection d'une option de paiement 324 parmi les options de paiement 831, 832. Ces moyens sont en particulier adaptés à fournir une liste des options de paiement 831, 832 présentes dans le champ M110 de la requête d'authentification M100. Ces moyens 360 de sélection d'une option de paiement sont également adaptés à stocker, dans un registre de la mémoire vive 320, l'option de paiement 324 retenue par l'utilisateur.

Le dispositif d'authentification 300 comporte également des moyens 370 de contrôle de l'identité de l'utilisateur. Ces moyens sont par exemple adaptés à vérifier, de façon connue, un numéro d'identification personnel (PIN) 344 stocké dans un registre de la mémoire non volatile 340. Ces moyens 370 de contrôle de l'identité de l'utilisateur sont également adaptés à bloquer le dispositif d'authentification 300 lorsque l'utilisateur saisit, à trois reprises, un numéro d'identification personnel différent du numéro d'identification personnel 344. Le dispositif 300 peut alors être débloqué par la saisie d'un numéro d'identification personnel de déblocage 346, stocké dans la mémoire non volatile 340.

Ce numéro d'identification personnel de déblocage 346 et la première clef d'authentification 342 sont respectivement reçus par le dispositif

d'authentification 300 dans les champs M410 et M420 d'un message de livraison de clefs M400 représenté sur la **figure 4**. Le message de livraison de clefs M400 comporte enfin un troisième code d'authentification M430 similaire au premier code d'authentification M130 de la requête d'authentification M100.

De retour à la figure 3, les moyens 330 de vérification sont également adaptés à vérifier la validité du message de livraison de clef M400, à partir du troisième code d'authentification. Le dispositif d'authentification 300 comporte également des moyens 380 d'envoi d'un message retour d'authentification M200, tel que décrit précédemment en référence à la figure 2.

Ces moyens 380 d'envoi d'un message retour d'authentification sont adaptés à incrémenter, avant chaque envoi d'un message retour d'authentification M200, un compteur de transactions 348, contenu dans un registre de la mémoire non volatile 340.

Ils sont également adaptés à générer un deuxième code d'authentification 326 et à le stocker dans un registre de la mémoire vive 320.

Les moyens 380 d'envoi d'un message retour d'authentification M200 sont aussi adaptés à construire un tel message, à partir de la réponse utilisateur 322, de l'option de paiement 324, du compteur de transactions 348 et du deuxième code d'authentification 326, ces valeurs remplissant respectivement les champs M210, M220, M230 et M240.

Les moyens 380 d'envoi d'un message retour d'authentification sont également adaptés à envoyer un message M200 à destination d'un serveur d'authentification 900, tel que décrit ultérieurement en référence à la figure 9.

Le dispositif d'authentification 300 comporte également des moyens de chiffrement et de déchiffrement 390, adaptés respectivement à chiffrer un message retour d'authentification M200 et à déchiffrer une requête d'authentification M100, à partir d'une clef de transport 349 stockée dans un registre de la mémoire non volatile 340. Cette clef de transport 349 est fournie au moment de la personnalisation du dispositif d'authentification 300.

La **figure 5** représente un serveur d'activation 500 selon l'invention. Un serveur d'activation 500 comporte des moyens 510 de réception

d'une requête d'activation M600 représentée sur la **figure 6**. Une telle requête d'activation M600 comporte un champ M610 contenant un identificateur d'un dispositif d'authentification 300. Sur réception d'une requête d'activation M600, les moyens 510 de réception lisent l'identificateur 522 d'un dispositif d'authentification 300 dans le champ M610 de cette requête d'activation M600 et le stockent dans un registre 522 d'une mémoire vive (RAM) 520. La requête d'activation M600 provient d'un serveur de comptes utilisateurs 800 qui sera décrit ultérieurement en référence à la figure 8.

De retour à la figure 5, le serveur d'activation 500 comporte également des moyens 530 de génération d'une clef d'authentification. Ces moyens 530 de génération d'une clef d'authentification sont en particulier adaptés à générer la première clef d'authentification 342 décrite en référence à la figure 3.

Ils sont également adaptés, dans un autre mode de réalisation, à générer une deuxième clef d'authentification 542, à partir de la première clef d'authentification 342.

Ces moyens 530 de génération d'une clef d'authentification sont également adaptés à stocker les clefs d'authentification 342 et 542 générées dans une base de données sécurisée 540.

Le serveur d'activation comporte également des moyens 550 d'envoi de message. Ces moyens 550 d'envoi de message sont en particulier adaptés à envoyer une requête d'activation M600 telle que représentée sur la figure 6.

Les moyens 550 d'envoi de message sont également adaptés à construire et à envoyer, au dispositif d'authentification 300, sur réception d'une réponse à la requête d'activation M600, un message M400 de livraison de clefs, tel que décrit en référence à la figure 4. Pour construire ce message, ils écrivent tout d'abord un numéro d'identification personnel de déblocage 346, lu dans une base de données de pré-activation 560, dans le champ M410 du message de livraison de clefs M400. Les moyens 550 d'envoi de message placent ensuite la première clef d'authentification 342 dans le champ M420, puis génèrent un troisième code d'authentification et le placent dans le champ M430.

Dans un mode préféré de réalisation, le message de livraison de clefs M400 est chiffré par des moyens de chiffrement 570 du serveur d'activation 500, avant l'envoi par les moyens d'envoi 550. Les moyens de chiffrement 570 utilisent en particulier la clef de transport 349 lue dans la base de données de pré-activation 560. Dans un mode particulier de réalisation, la clef de transport 349 est également utilisée par les moyens 550 d'envoi de message pour générer le troisième code d'authentification.

Les moyens 550 d'envoi de message sont également adaptés à envoyer un enregistrement d'authentification M700 représenté sur la **figure 7** à un serveur d'authentification 900 décrit plus loin en référence à la figure 9. L'enregistrement d'authentification M700 comporte deux champs M710 et M720 destinés respectivement à contenir la clef de transport 349 et le numéro d'identification personnel de déblocage 346.

La requête d'activation M600, le message M400 de livraison de clefs et l'enregistrement d'authentification M700 peuvent être mémorisés dans la mémoire vive 520 du serveur d'activation 500.

La **figure 8** représente un serveur de comptes utilisateurs 800 selon l'invention. Un serveur de comptes utilisateurs 800 comporte des moyens 810 de création de comptes utilisateurs. Ces moyens de création 810 sont en particulier adaptés à créer un compte utilisateur 830 et à le stocker dans une zone de stockage 820.

Un compte utilisateur 830 comporte un identificateur 522 d'un dispositif d'authentification 300 et différentes options de paiement 831, 832.

Le serveur de comptes utilisateurs 800 comporte également des moyens 840 d'envoi d'une requête. Ces moyens 840 d'envoi d'une requête sont en particulier adaptés à envoyer une requête d'activation M600, telle que décrite en référence à la figure 6, à destination d'un serveur d'activation 500. Ils sont également adaptés à envoyer une deuxième requête d'authentification à destination d'un serveur d'authentification 900 qui va maintenant être décrit.

La **figure 9** représente un serveur d'authentification 900 selon l'invention. Un serveur d'authentification 900 comporte des moyens 910 de réception d'un enregistrement d'authentification M700 en provenance d'un

serveur d'activation 500. Ces moyens de réception 910 sont adaptés à stocker un enregistrement d'authentification M700 reçu dans une zone de stockage d'enregistrements d'authentification 920.

Les moyens de réception 910 sont également adaptés à recevoir une deuxième requête d'authentification en provenance d'un serveur de comptes utilisateurs 800.

Le serveur d'authentification 900 comporte des moyens d'envoi 930 adaptés à envoyer une première requête d'activation M100, décrite en relation avec la figure 1, à destination d'un dispositif d'authentification 300. Les moyens de réception 910 sont également adaptés à recevoir un message retour d'authentification M200 en provenance du dispositif d'authentification 300. Les moyens d'envoi 930 sont enfin adaptés à envoyer un message de confirmation de transaction (non représenté ici), à destination d'un serveur de comptes utilisateurs 800.

La **figure 10** représente un système 10 de paiement électronique à distance selon l'invention. Un tel système 10 comporte un dispositif d'authentification 300, un serveur d'activation 500, un serveur de comptes utilisateurs 800 et un serveur d'authentification 900. Dans le mode de réalisation décrit ici, le dispositif d'authentification 300 est incorporé dans une carte SIM 20 adaptée à être insérée dans une fente 32 d'un téléphone portable 30. Le système 10 de paiement électronique à distance utilise une infrastructure d'un réseau 40 de télécommunications mobiles de type GSM pour le transport des requêtes d'authentification M100, des messages retour d'authentification M200, des messages de livraison de clefs M400 et des requêtes d'activation M600. Plus précisément, les messages et requêtes M100, M200, M400 et M600 sont conformes au format SMS du protocole GSM. Le téléphone portable 30 comporte en outre des moyens de saisie 34, par exemple sous forme d'un clavier, d'un numéro d'identification personnel 344. Dans ce mode de réalisation, l'identificateur 522 du dispositif d'authentification 300 est le numéro de téléphone du téléphone mobile 30, associé à la carte SIM 20.

La **figure 11** représente un organigramme d'un procédé d'authentification selon l'invention.

Un procédé d'authentification selon l'invention comporte une première étape E1100 de réception d'un message M400 de livraison de clefs. Ce message de livraison de clefs M400 est reçu en provenance d'un serveur d'activation 500. Ce message M400 contient une clef d'authentification 342, un numéro d'identification personnel de déblocage 346 et un troisième code d'authentification dans un champ M430.

L'étape E1100 est suivie par un test E1110 au cours duquel la validité du message de livraison de clefs M400 est vérifiée. Cette vérification utilise en particulier le troisième code d'authentification reçu au cours de l'étape E1100.

Lorsque ce message de livraison de clefs n'est pas valide, le résultat du test E1110 est négatif. Ce test est alors suivi par une étape E1120 au cours de laquelle un message d'information est envoyé au serveur d'activation 500.

Dans le cas où le message de livraison de clefs M400 est valide, le résultat du test E1110 est positif. Ce test est alors suivi par une étape E1130 de réception d'une première requête d'authentification M100 en provenance d'un serveur d'authentification 900. Cette première requête d'authentification comporte, entre autres, une description de la transaction et un premier code d'authentification.

Cette étape E1130 est suivie par une étape E1135 de création d'un message retour d'authentification M200, dont les champs M210, M220, M230 et M240 sont vides.

L'étape E1135 est suivie par une étape E1140 de déchiffrement de la première requête d'authentification M100, reçue au cours de l'étape E1130. Cette étape de déchiffrement E1140 utilise une clef de transport 349, typiquement fournie lors d'une étape de personnalisation non représentée ici.

L'étape E1140 est suivie par un test E1150 au cours duquel la validité de la requête d'authentification est testée. Ce test E1150 utilise en particulier le premier code d'authentification contenu dans le champ M130 de la requête d'authentification reçue à l'étape E1130, ainsi que la première clef d'authentification 342.

Lorsque cette requête n'est pas valide, le résultat du test E1150 est négatif. Ce test est alors suivi par une étape E1160, au cours de laquelle le champ M210 du message retour d'authentification M200 créé à l'étape E1135 est initialisé avec un code d'erreur « MAC_NG » représentatif de la réception d'une requête d'authentification non valide. L'étape E1160 est alors suivie par une étape E1270 qui sera décrite ultérieurement.

Lorsque la requête d'authentification M100 est valide, le résultat du test E1150 est positif. Ce test est alors suivi par un test E1170 au cours duquel l'identité de l'utilisateur est vérifiée. De façon connue, l'étape E1170 consiste à comparer un numéro d'identification personnel saisi par l'utilisateur, avec un numéro d'identification personnel 344, par exemple reçu par courrier. Dans le cas où l'utilisateur saisit un numéro d'identification personnel erroné, par exemple à trois reprises, le résultat du test E1170 est négatif. Ce test est alors suivi par une étape E1180 au cours de laquelle le champ M210 du message retour d'authentification M200 créé à l'étape E1135 est initialisé avec un code d'erreur « PIN_NG » représentatif d'un utilisateur non valide. L'étape E1180 est alors suivie par une étape E1270 qui sera décrite ultérieurement.

Lorsque l'utilisateur saisit un numéro d'identification personnel identique au numéro d'identification personnel 344, le résultat du test E1170 est positif. Ce test est alors suivi par une étape E1190. Au cours de cette étape, l'utilisateur accepte ou refuse la transaction décrite dans le champ M110 de la requête d'authentification M100 reçue à l'étape E1130.

Lorsque cette transaction est refusée, une variable « Réponse » 322 est initialisée avec la valeur NG et l'étape E1190 est suivie par une étape E1220 qui sera décrite ultérieurement.

Lorsque cette transaction est acceptée, la variable « Réponse » 322 est initialisée avec la valeur OK. L'étape E1190 est dans ce cas suivie par une étape E1200 de sélection d'une option de paiement 324. Cette option de paiement 324 est choisie parmi différentes options de paiement 831, 832 contenues dans le champ M110 de la requête d'authentification M100 reçue à l'étape E1130.

Cette option de paiement est ensuite insérée au cours de l'étape E1210 dans le champ M220 du message retour d'authentification M200 créé à l'étape E1135.

L'étape E1210 est suivie par une étape E1220, au cours de laquelle la valeur de la variable « Réponse » 322 est insérée dans le champ M210 du message retour d'authentification M200 créé à l'étape E1135.

L'étape E1220 est suivie par une étape E1230, au cours de laquelle un compteur de transactions 348 est incrémenté. La valeur de ce compteur de transactions 348 est insérée, au cours de l'étape suivante E1240, dans le champ M230 du message retour d'authentification M200 créé à l'étape E1135.

L'étape E1240 est suivie par une étape E1250 de génération d'un deuxième code d'authentification, inséré au cours de l'étape suivante E1260 dans le champ M240 du message retour d'authentification créé à l'étape E1135.

L'étape E1260 est suivie par une étape E1270 de chiffrement du message retour d'authentification M200 créé au cours de l'étape E1135. Cette étape E1270 de chiffrement de message utilise en particulier la clef de transport 349.

L'étape E1270 est suivie par une étape E1280 d'envoi du message retour d'authentification M200, à destination du serveur d'authentification 900, à l'origine de la requête d'authentification M100 reçue au cours de l'étape E1130.

REVENDICATIONS

1. Dispositif d'authentification (300) auprès d'un serveur d'authentification (900) dans un système de paiement à distance (10), ladite authentification étant préalable à une transaction par un utilisateur, ledit dispositif (300) étant caractérisé en ce qu'il comporte :

-des moyens (310) de réception d'une première requête d'authentification (M100), en provenance dudit serveur d'authentification (900) ;

-des moyens (330) de vérification de la validité de ladite requête d'authentification (M100) ;

-des moyens (350) de validation, par l'utilisateur, de ladite transaction ;

-des moyens (370) de contrôle de l'identité dudit utilisateur ; et

-des moyens (380) d'envoi d'un message retour d'authentification (M200), vers ledit serveur d'authentification (900).

2. Dispositif d'authentification (300) selon la revendication 1, ladite requête d'authentification (M100) comprenant une description de ladite transaction, un identifiant de ladite transaction et un premier code d'authentification dudit serveur d'authentification (900), ledit dispositif (300) étant caractérisé en ce que lesdits moyens (330) de vérification sont adaptés à vérifier la validité de ladite requête d'authentification (M100) à partir dudit premier code d'authentification et d'une première clef d'authentification (342).

3. Dispositif d'authentification (300) selon la revendication 1 ou 2, caractérisé en ce qu'il comporte en outre des moyens (380) de génération d'un deuxième code d'authentification (326), et en ce que lesdits moyens (380) d'envoi du message retour d'authentification (M200) sont adaptés à insérer ledit deuxième code d'authentification (326) dans ledit message retour d'authentification (M240).

4. Dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 3, caractérisé en ce que lesdits moyens (380) d'envoi du message retour d'authentification (M200) sont adaptés à insérer une réponse

(322) dans ledit message retour d'authentification (M200), ladite réponse (322) étant fonction de ladite validation de la transaction.

5. Dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 4, caractérisé en ce que lesdits moyens (370) de contrôle de l'identité dudit utilisateur utilisent un numéro d'identification personnel (344).

6. Dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comporte en outre des moyens (390) de déchiffrement de ladite première requête d'authentification (M100), à partir d'une clef de transport (349).

7. Dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comporte en outre des moyens (390) de chiffrement dudit message retour d'authentification (M200), à partir d'une clef de transport (349).

8. Dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 7, ladite transaction comportant une opération de paiement, ledit dispositif étant caractérisé en ce qu'il comporte en outre des moyens (360) de sélection d'une option de paiement (324) de ladite transaction et en ce que lesdits moyens (380) d'envoi du message retour d'authentification (M200) sont adaptés à insérer ladite option (324) dans ledit message retour d'authentification (M220).

9. Dispositif d'authentification (300) selon l'une quelconque des revendications 3 à 8, caractérisé en ce qu'il comporte en outre un compteur de transactions (348) utilisé par lesdits moyens (380) de génération dudit deuxième code d'authentification (326), et en ce que lesdits moyens (380) d'envoi du message retour d'authentification (M200) sont adaptés à insérer ledit compteur de transactions (348) dans ledit message retour d'authentification (M230).

10. Dispositif d'authentification (300) selon l'une quelconque des revendications 2 à 9, caractérisé en ce qu'il comporte en outre des moyens (310) de réception, en provenance d'un serveur d'activation (500), d'un message de livraison de clefs (M400), ledit message de livraison de clefs (M400) comportant ladite première clef d'authentification (342).

11. Dispositif d'authentification (300) selon la revendication 10, caractérisé en ce ledit message de livraison de clefs (M400) comporte en outre un numéro d'identification personnel de déblocage (346).

12. Dispositif d'authentification (300) selon la revendication 10 ou 11, caractérisé en ce qu'il comporte en outre des moyens (330) de vérification de la validité dudit message de livraison de clefs (M400), à partir d'un troisième code d'authentification contenu dans ledit message de livraison de clefs (M430).

13. Carte à puce, caractérisée en ce qu'elle comporte un dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 12.

14. Carte SIM (20), caractérisée en ce qu'elle comporte un dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 12.

15. Téléphone (30), caractérisé en ce qu'il comporte des moyens (32) adaptés à recevoir une carte SIM (20) selon la revendication 14.

16. Téléphone (30) selon la revendication 15, la carte SIM (20) comportant un dispositif d'authentification (300) selon l'une quelconque des revendications 5 à 12, ledit téléphone (30) étant caractérisé en ce qu'il comporte en outre des moyens (34) de saisie dudit numéro d'identification personnel (344).

17. Serveur d'activation (500), dans un système de paiement à distance (10), caractérisé en ce qu'il comporte :

-des moyens (510) de réception d'une requête d'activation (M600) en provenance d'un serveur de comptes d'utilisateurs (800), ladite requête d'activation (M600) comportant un identificateur (522) d'un dispositif d'authentification (300) selon l'une quelconque des revendications 10 à 12 ;

-des moyens (530) de génération de ladite première clef d'authentification (342) ; et

-des moyens (550) d'envoi, sur réception d'une réponse à ladite requête d'activation (M600), dudit message de livraison de clefs (M400) audit dispositif d'authentification (300).

18. Serveur d'activation (500) selon la revendication 17, caractérisé en ce que ledit identificateur (522) est un numéro de téléphone.

19. Serveur d'activation (500) selon la revendication 17 ou 18, caractérisé en ce qu'il comporte en outre des moyens (530) de sauvegarde de ladite première clef d'authentification (342) dans une base de données sécurisée (540).

20. Serveur d'activation (500) selon l'une quelconque des revendications 17 à 19, caractérisé en ce qu'il comporte en outre des moyens (530) de génération d'une deuxième clef d'authentification (542), à partir de ladite première clef d'authentification (342) et en ce qu'il comporte des moyens de sauvegarde (530) de ladite deuxième clef d'authentification (542) dans une base de données sécurisée (540).

21. Serveur d'activation (500) selon l'une quelconque des revendications 17 à 20, caractérisé en ce qu'il comporte en outre des moyens (550) de calcul d'un troisième code d'authentification, et en ce que lesdits moyens d'envoi (550) sont adaptés à insérer ledit troisième code d'authentification dans ledit message de livraison de clefs (M430).

22. Serveur d'activation (500) selon l'une quelconque des revendications 17 à 21, ladite requête d'activation (M600) comportant un identificateur d'un dispositif d'authentification (522) selon la revendication 11 ou 12, ledit serveur d'activation (500) étant caractérisé en ce que lesdits moyens (550) d'envoi sont adaptés à insérer ledit numéro d'identification personnel de déblocage (346) dans ledit message de livraison de clefs (M410).

23. Serveur d'activation (500) selon la revendication 21, caractérisé en ce qu'il comporte en outre des moyens (570) de chiffrement dudit message de livraison de clefs (M400), à partir d'une clef de transport (349).

24. Serveur d'activation (500) selon la revendication 23, caractérisé en ce qu'il comporte en outre des moyens (550) d'obtention de ladite clef de transport (349) et d'un numéro d'identification personnel de déblocage (346) à partir d'une base de données de pré-activation (560).

25. Serveur d'activation (500) selon la revendication 23 ou 24, caractérisé en ce que lesdits moyens (550) de calcul sont adaptés à calculer ledit troisième code d'authentification à partir de ladite clef de transport (349).

26. Serveur d'activation (500) selon la revendication 24 ou 25, caractérisé en ce qu'il comporte en outre des moyens (550) d'envoi d'un enregistrement d'authentification (M700), à destination d'un serveur d'authentification (900), ledit enregistrement d'authentification (M700) comportant ladite clef de transport (349) et ledit numéro d'identification personnel de déblocage (346).

27. Serveur de comptes utilisateurs (800), dans un système de paiement à distance (10), caractérisé en ce qu'il comporte :

-des moyens (810) de création et de stockage d'au moins un compte utilisateur (830) associé à un dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 12 ;

-des moyens (840) d'envoi d'une requête d'activation (M600), à destination d'un serveur d'activation (500) selon l'une quelconque des revendications 17 à 26 ; et

-des moyens (840) d'envoi d'une deuxième requête d'authentification à destination d'un serveur d'authentification (900).

28. Serveur de comptes utilisateurs (800) selon la revendication 27, caractérisé en ce que ledit compte utilisateur comporte :

-un identificateur (522) dudit dispositif d'authentification (300) ; et

-au moins une option de paiement (831, 832) de ladite transaction.

29. Serveur d'authentification (900), dans un système de paiement à distance (10), caractérisé en ce qu'il comporte :

-des moyens (910) de réception d'au moins un enregistrement d'authentification (M700) en provenance d'un serveur d'activation (500) selon la revendication 26 ;

-des moyens (910) de stockage dudit enregistrement d'authentification (M700) ;

-des moyens (910) de réception d'une deuxième requête d'authentification en provenance d'un serveur de comptes utilisateurs (800) selon la revendication 27 ou 28 ;

-des moyens (930) d'envoi de ladite première requête d'authentification (M100), à destination d'un dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 12, sur réception de ladite deuxième requête d'identification;

-des moyens (910) de réception d'un message retour d'authentification (M200), en provenance dudit dispositif d'authentification (300) ; et

-des moyens (930) d'envoi d'un message de confirmation de transaction audit serveur de comptes utilisateurs (800), sur réception dudit message retour d'authentification (M200).

30. Système de paiement à distance (10), caractérisé en ce qu'il comporte un dispositif d'authentification (300) selon l'une quelconque des revendications 1 à 12, un serveur d'activation (500) selon l'une quelconque des revendications 17 à 26, un serveur de comptes utilisateurs (800) selon la revendication 27 ou 28 et un serveur d'authentification (900) selon la revendication 29.

31. Système de paiement à distance (10) selon la revendication 30, caractérisé en ce qu'il utilise une infrastructure d'un réseau (40) de téléphonie mobile.

32. Système de paiement à distance (10) selon la revendication 31, caractérisé en ce que ledit réseau mobile (40) est un réseau GSM.

33. Système de paiement à distance (10) selon la revendication 32, caractérisé en ce que lesdits messages et lesdites requêtes sont conformes au format SMS du protocole GSM.

34. Procédé d'authentification auprès d'un serveur d'authentification (900) dans un système de paiement à distance (10), ladite authentification étant préalable à une transaction par un utilisateur, ledit procédé étant caractérisé en ce qu'il comporte les étapes suivantes :

-réception (E1130) d'une première requête d'authentification (M100), en provenance dudit serveur d'authentification (900);

-vérification (E1150) de la validité de ladite requête d'authentification (M100);

-validation (E1190), par l'utilisateur, de ladite transaction ;

-contrôle (E1170) de l'identité dudit utilisateur ; et

-envoi (E1280) d'un message retour d'authentification (M200), vers ledit serveur d'authentification (900).

35. Procédé d'authentification selon la revendication 34, ladite requête d'authentification (M100) comprenant une description de ladite transaction, un identifiant de ladite transaction et un premier code d'authentification dudit serveur d'authentification (900), ledit procédé étant caractérisé en ce que la validité de ladite requête d'authentification est vérifiée en utilisant ledit premier code d'authentification et une première clef d'authentification (342), au cours de ladite étape de vérification (E1150).

36. Procédé d'authentification selon la revendication 34 ou 35, caractérisé en ce qu'il comporte en outre une étape (E1250) de génération d'un deuxième code d'authentification, ledit deuxième code d'authentification étant inséré dans ledit message retour d'authentification (M240) au cours d'une première étape d'insertion (E1260).

37. Procédé d'authentification selon l'une quelconque des revendications 34 à 36, caractérisé en ce qu'une réponse (322), dépendante de ladite validation de la transaction, est insérée dans ledit message retour d'authentification (M210) au cours d'une deuxième étape d'insertion (E1220).

38. Procédé d'authentification selon l'une quelconque des revendications 34 à 37, caractérisé en ce qu'un numéro d'identification personnel (344) est utilisé au cours de ladite étape de contrôle de l'identité dudit utilisateur (E1170).

39. Procédé d'authentification selon l'une quelconque des revendications 34 à 38, caractérisé en ce qu'il comporte en outre une étape (E1140) de déchiffrement de ladite première requête d'authentification (M100), à partir d'une clef de transport (349).

40. Procédé d'authentification selon l'une quelconque des revendications 34 à 39, caractérisé en ce qu'il comporte en outre une étape de chiffrement (E1270) dudit message retour d'authentification (M200), à partir d'une clef de transport (349).

41. Procédé d'authentification selon l'une quelconque des revendications 34 à 40, ladite transaction comportant une opération de paiement, ledit procédé étant caractérisé en ce qu'il comporte en outre une étape (E1200) de sélection d'une option de paiement (324) de ladite transaction, ladite option (324) étant insérée dans ledit message retour d'authentification (champ M220 de M200) au cours d'une étape (E1210) d'insertion d'une option de paiement.

42. Procédé d'authentification selon l'une quelconque des revendications 36 à 41, caractérisé en ce que ladite étape (E1250) de génération dudit deuxième code d'authentification utilise un compteur de transactions (348), ledit compteur de transactions (348) étant inséré dans ledit message retour d'authentification (M230), au cours d'une étape (E1240) d'insertion d'un compteur de transactions.

43. Procédé d'authentification selon l'une quelconque des revendications 35 à 42, caractérisé en ce qu'il comporte en outre une étape (E1100) de réception d'un message de livraison de clefs (M400), ledit message de livraison de clefs (M400) comportant ladite première clef d'authentification (342).

44. Procédé d'authentification selon la revendication 43, caractérisé en ce que ledit message de livraison de clefs (M400) comporte en outre un numéro d'identification personnel de déblocage (346).

45. Procédé d'authentification selon la revendication 43 ou 44, caractérisé en ce qu'il comporte en outre une étape (E1110) de vérification de la validité dudit message de livraison de clefs (M400), à partir d'un troisième code d'authentification contenu dans ledit message de livraison de clefs (M430).

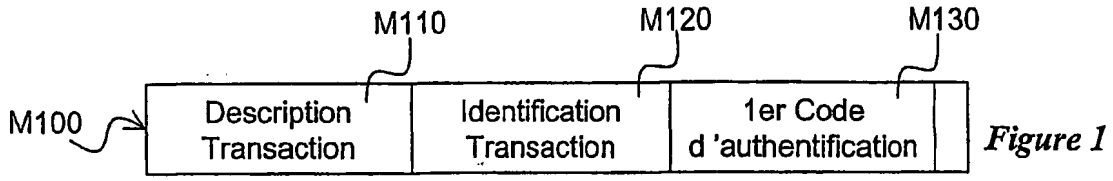


Figure 1

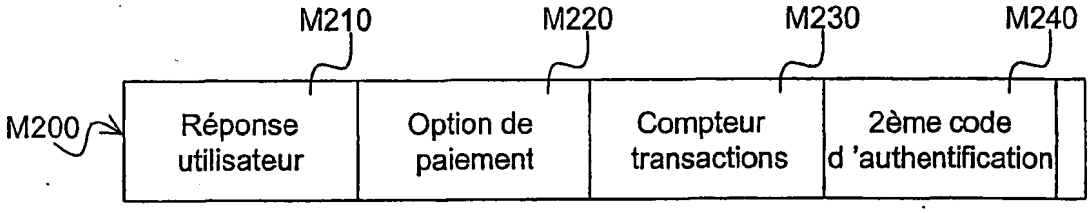


Figure 2

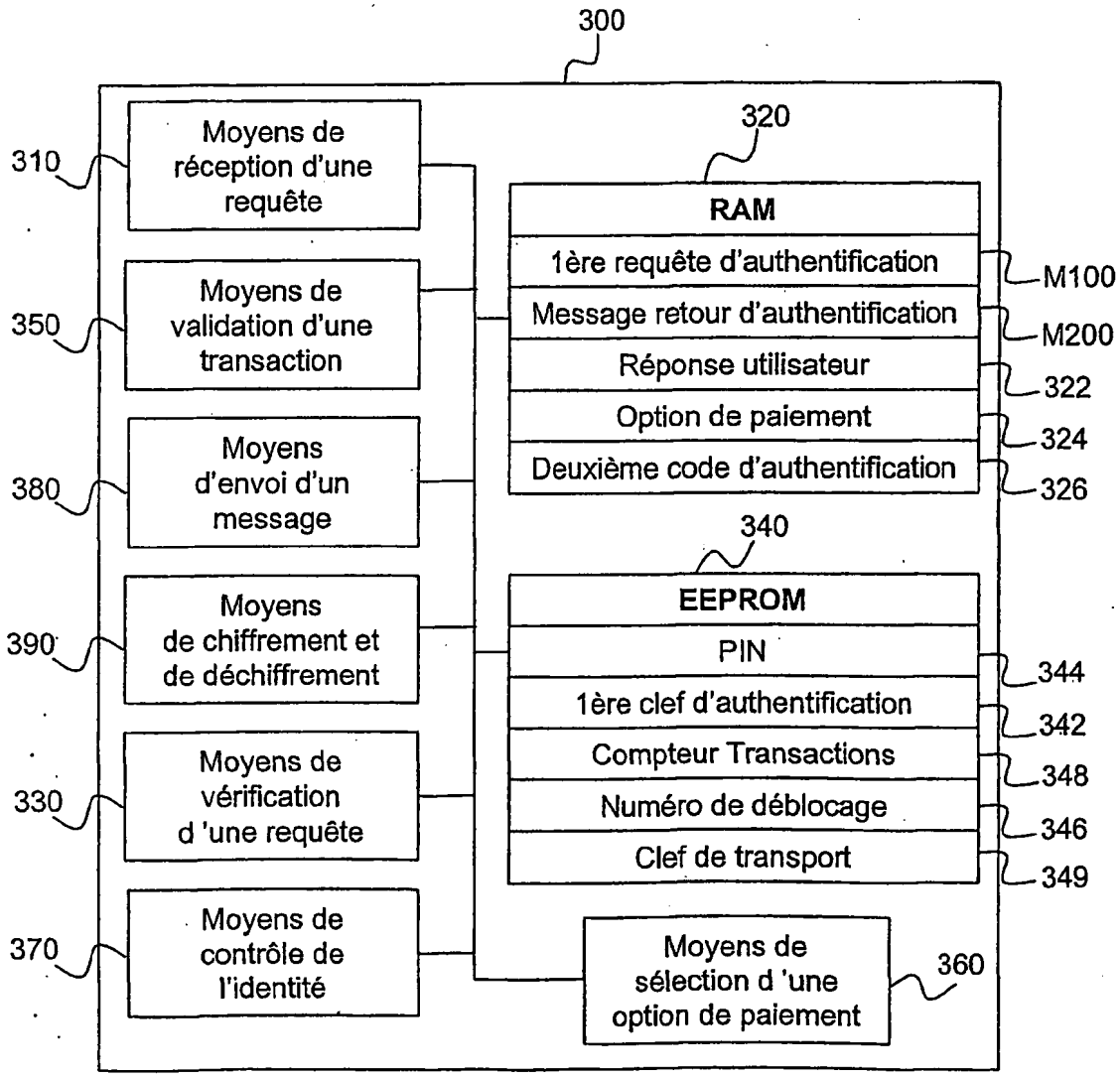


Figure 3

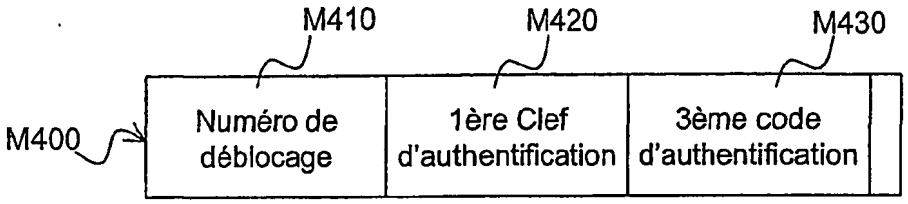


Figure 4

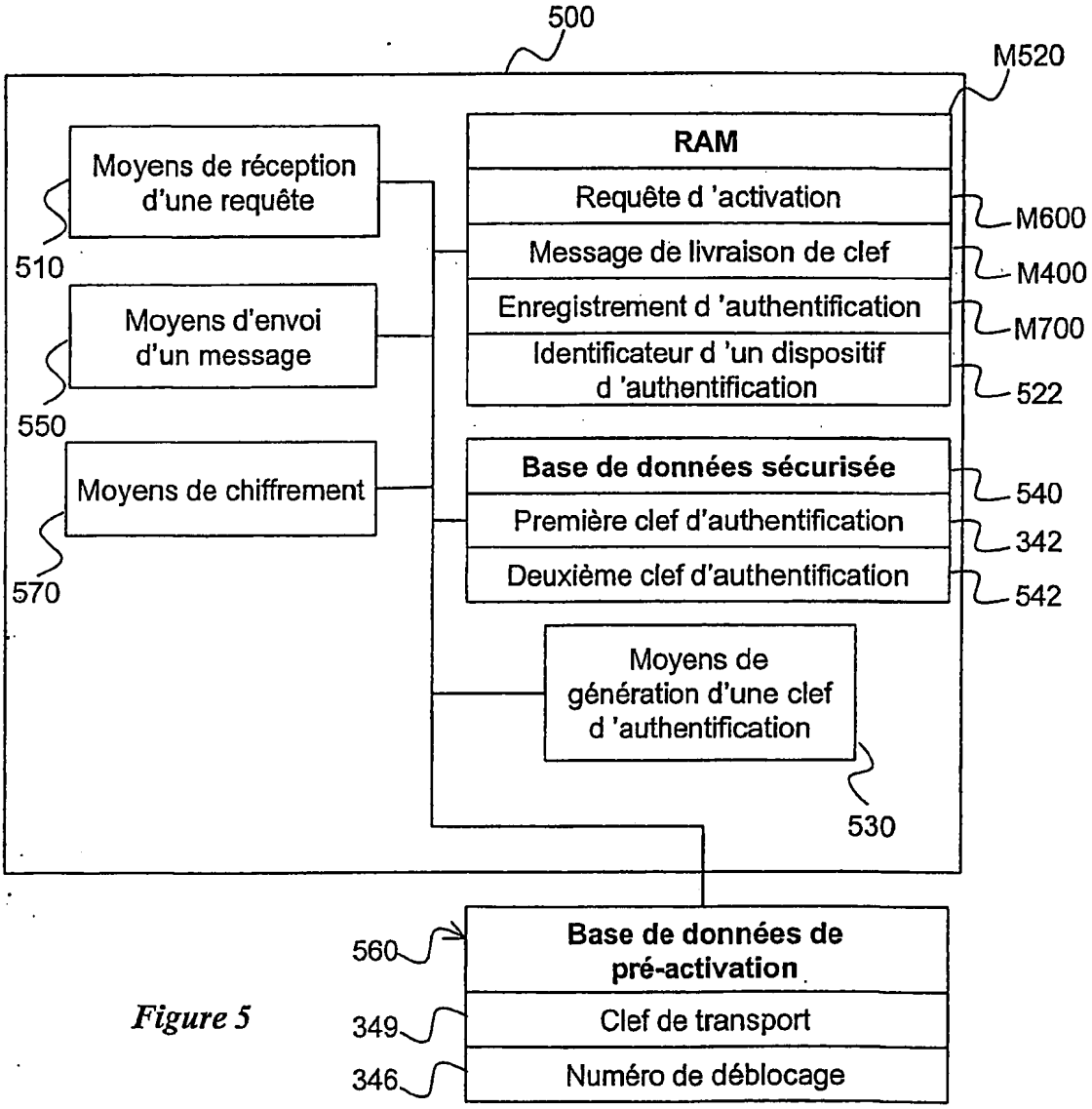


Figure 5

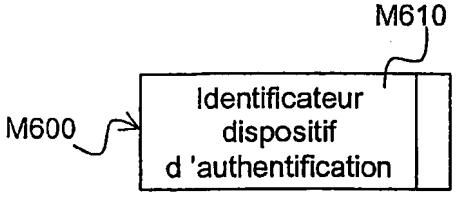


Figure 6

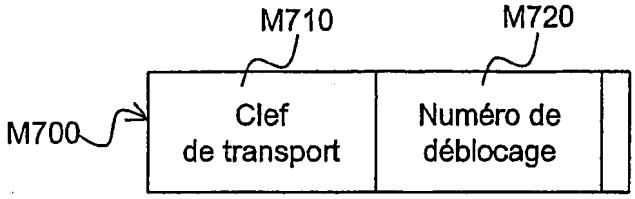


Figure 7

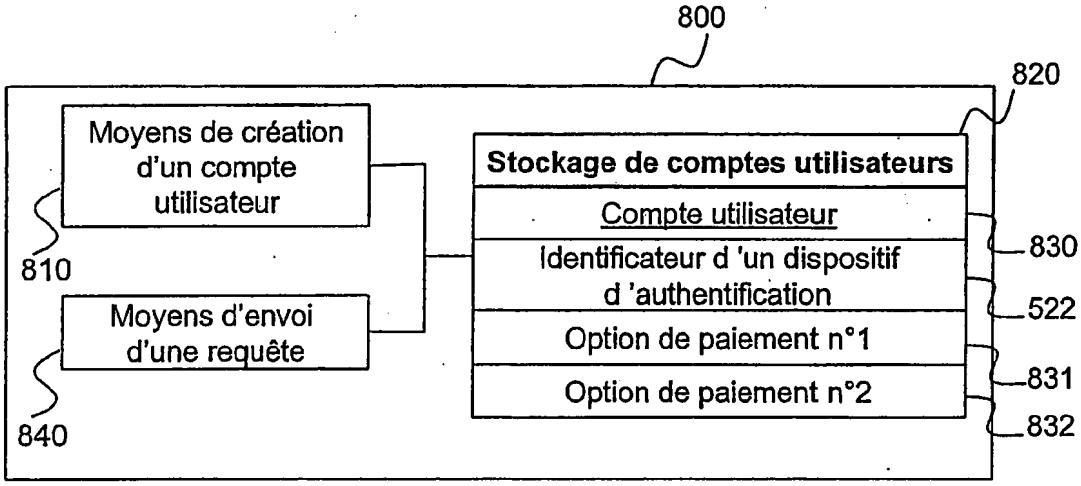


Figure 8

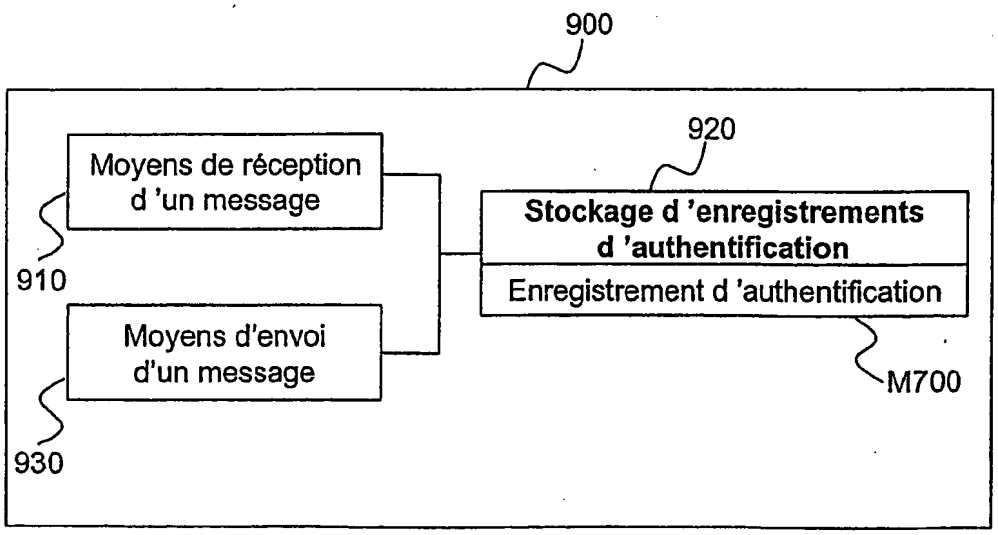


Figure 9

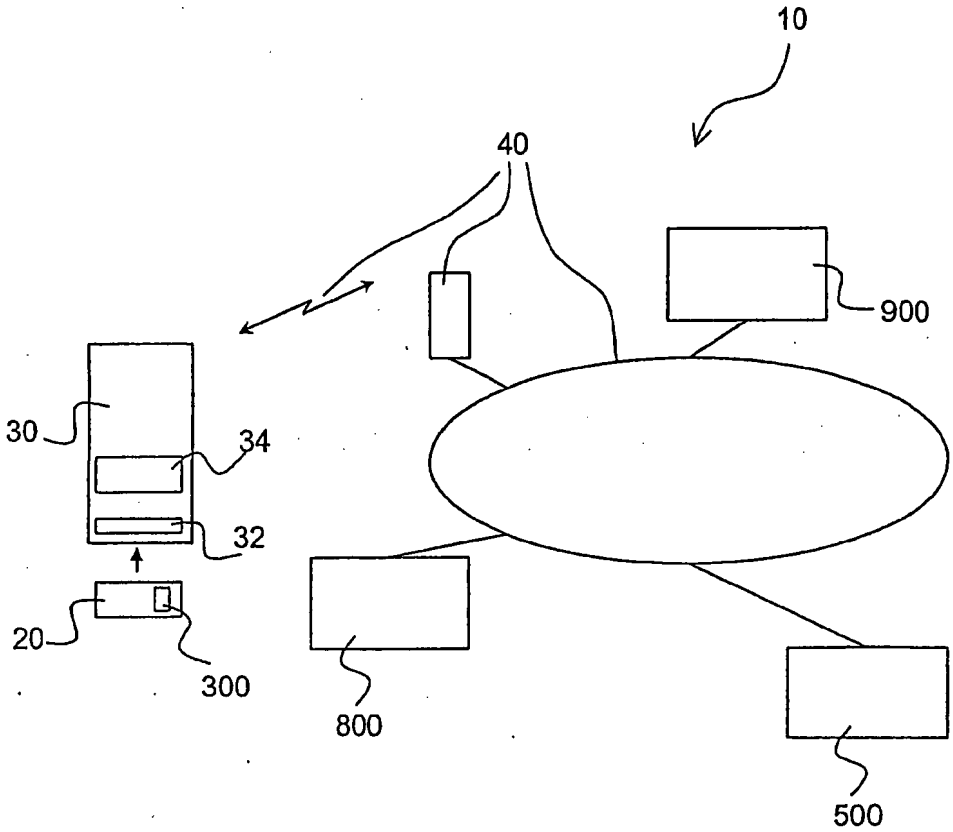


Figure 10

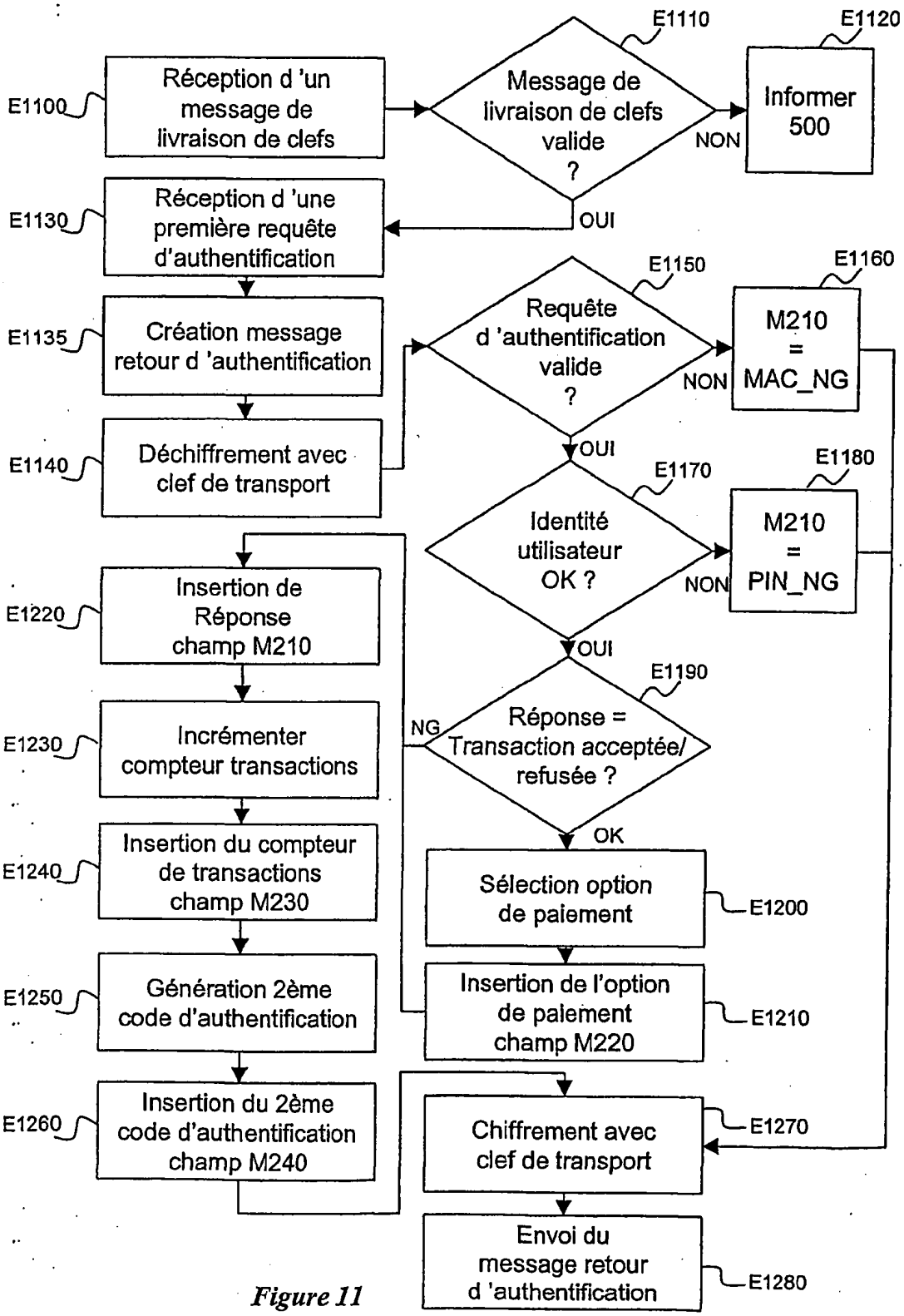

E1100
Réception d 'un message de livraison de clefs
E1110
Message de livraison de clefs valide ?
NON
E1120
Informer 500
OUI
E1130
Réception d 'une première requête d'authentification
E1135
Création message retour d 'authentification
E1140
Déchiffrement avec clef de transport
E1150
Requête d 'authentification valide ?
NON
E1160
M210 = MAC_NG
OUI
E1170
Identité utilisateur OK ?
NON
E1180
M210 = PIN_NG
OUI
E1190
Réponse = Transaction acceptée/ refusée ?
NG
OK
E1200
Sélection option de paiement
E1210
Insertion de l'option de paiement champ M220
E1220
Insertion de Réponse champ M210
E1230
Incrémenter compteur transactions
E1240
Insertion du compteur de transactions champ M230
E1250
Génération 2ème code d'authentification
E1260
Insertion du 2ème code d'authentification champ M240
E1270
Chiffrement avec clef de transport
E1280
Envoi du message retour d 'authentification

Figure 11

INTERNATIONAL SEARCH REPORT

In ional Application No
PCT/FR 02/00626

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 406 628 A (BELLER MICHAEL J ET AL) 11 April 1995 (1995-04-11)	1-4,6,7, 10, 13-15, 17, 34-37, 39,40,43
Y		5,6,11, 12,18, 38,44
A		7-9,16, 19-33, 39-42,45
	column 5, line 1-13 column 5, line 35-68 column 7, line 1-8 column 10, line 36 -column 11, line 2 column 11, line 10-40 column 11, line 58-68 claim 1 -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July 2002	31/07/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro, M.L.

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 784 463 A (CHEN JAMES F ET AL) 21 July 1998 (1998-07-21) column 5, line 28-39	5,6,11, 12,38,44
Y	EP 0 862 104 A (CASIO COMPUTER CO LTD) 2 September 1998 (1998-09-02) abstract	18
A	BRANDS S: "ELECTRONIC CASH ON THE INTERNET" PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, XX, XX, 1995, pages 64-84, XP000567597 page 73, left-hand column, line 32 -page 74, left-hand column, line 34	1-45

INTERNATIONAL SEARCH REPORT

Information on patent family members

In ional Application No
PCT/FR 02/00626

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5406628	A	11-04-1995	US	5299263 A	29-03-1994
			CA	2157011 A1	15-09-1994
			DE	69426416 D1	18-01-2001
			DE	69426416 T2	26-07-2001
			EP	0691055 A1	10-01-1996
			JP	8507619 T	13-08-1996
			WO	9421067 A1	15-09-1994
US 5784463	A	21-07-1998	AU	5588198 A	29-06-1998
			WO	9825375 A1	11-06-1998
EP 0862104	A	02-09-1998	JP	10243120 A	11-09-1998
			JP	11175477 A	02-07-1999
			CN	1193862 A	23-09-1998
			EP	0862104 A2	02-09-1998
			US	6108790 A	22-08-2000

RAPPORT DE RECHERCHE INTERNATIONALE

De de internationale No
PCT/FR 02/00626

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5 406 628 A (BELLER MICHAEL J ET AL) 11 avril 1995 (1995-04-11)	1-4,6,7, 10, 13-15, 17, 34-37, 39,40,43
Y		5,6,11, 12,18, 38,44
A		7-9,16, 19-33, 39-42,45
	colonne 5, ligne 1-13 colonne 5, ligne 35-68 colonne 7, ligne 1-8 colonne 10, ligne 36 -colonne 11, ligne 2 colonne 11, ligne 10-40 colonne 11, ligne 58-68 revendication 1 -/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
24 juillet 2002	31/07/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro, M.L.

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

De de internationale No
PCT/FR 02/00626

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 5 784 463 A (CHEN JAMES F ET AL) 21 juillet 1998 (1998-07-21) colonne 5, ligne 28-39	5,6,11, 12,38,44
Y	EP 0 862 104 A (CASIO COMPUTER CO LTD) 2 septembre 1998 (1998-09-02) abrégé	18
A	BRANDS S: "ELECTRONIC CASH ON THE INTERNET" PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, XX, XX, 1995, pages 64-84, XP000567597 page 73, colonne de gauche, ligne 32 -page 74, colonne de gauche, ligne 34	1-45

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

De le Internationale No
PCT/FR 02/00626

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5406628	A	11-04-1995	US	5299263 A	29-03-1994
			CA	2157011 A1	15-09-1994
			DE	69426416 D1	18-01-2001
			DE	69426416 T2	26-07-2001
			EP	0691055 A1	10-01-1996
			JP	8507619 T	13-08-1996
			WO	9421067 A1	15-09-1994
US 5784463	A	21-07-1998	AU	5588198 A	29-06-1998
			WO	9825375 A1	11-06-1998
EP 0862104	A	02-09-1998	JP	10243120 A	11-09-1998
			JP	11175477 A	02-07-1999
			CN	1193862 A	23-09-1998
			EP	0862104 A2	02-09-1998
			US	6108790 A	22-08-2000